

**REMARKS**

**I. INTRODUCTION**

Claims 1, 22, 25, and 26 have been amended to put the application in condition for allowance, or at least in better condition for appeal. Claims 11 and 33-36 were cancelled previously. The amendments made herein are fully consistent with and supported by the originally-filed disclosure. No new matter within the meaning of 35 U.S.C. 132(a) has been introduced by the foregoing amendments.

All of the outstanding claim rejections are traversed for the reasons set out below.

**II. THE CLAIM REJECTIONS UNDER 35 U.S.C. § 103(a) SHOULD BE WITHDRAWN**

The March 9, 2009 Final Office Action contained multiple rejections under 35 U.S.C. § 103(a), namely:

- a rejection of claims 1-2, 5-9, 12-19, 22-26, and 29-32<sup>1</sup> as being unpatentable for obviousness over Saito et al. “Privacy Enhanced Access Control by SPKI” (hereinafter “Saito”) in view of U.S. Patent No, 5,717,758 to Micall (hereinafter “Micall”);
- a rejection of claims 3-4, 10, 20-21, and 27-28<sup>2</sup> as being unpatentable for obviousness over Saito in view of Micall, and further in view of U.S. Patent Application Publication No. 2007/0189542 to Alldredge (hereinafter “Alldredge”).

Such rejections are traversed.

In the March 9, 2009 Final Office Action, the examiner conceded that “Saito does not disclose reissuing associations between user identifying information and data” (March 9, 2009 Office Action, page 2), but alleged that it would be obvious to combine Micall with Saito to yield the subject matter of Applicants’ independent claims. As detailed below, Saito relates to Simple Public Key Infrastructure (SPKI), while Micall relates to Public Key Infrastructure

---

<sup>1</sup> See 03/09/09 Office Action, pp. 2-9.

<sup>2</sup> See 09/09/09 Office Action, pp. 9-11.

(“PKI”), such that Micall is not properly combinable with Saito to support the rejection of any of Applicants’ independent claims. The distinctions between PKI and SPKI are discussed below to provide appropriate background for the impropriety of combining the disclosures of Micall and Saito.

A. Discussion of Public Key Infrastructure (PKI) and Simple Public Key Infrastructure (SPKI)

It is generally understood in the art that both Public Key Infrastructure (“PKI”) and Simple Public Key Infrastructure (“SPKI”) represent different authentication solutions, with PKI utilizing a certificate authority (CA) that binds public keys with user identities, but with SPKI eliminating the need for any certificate authority by use of an authorization loop (whereby the verifier is also the issuer (such that public authentication of public key information, and use of a certificate authority, is *unnecessary*). See, e.g., discussion of Public Key Infrastructure and Simple Public Key Infrastructure from Wikipedia, as reproduced in pertinent part below.

“A Public Key Infrastructure (**PKI**) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. A PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique for each CA. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). For each user, the user identity, the public key, their binding, validity conditions and other attributes are made unforgeable in public key certificates issued by the CA. The term trusted third party (TTP) may also be used for certificate authority (CA).”

(See [http://en.wikipedia.org/wiki/Public\\_key\\_infrastructure](http://en.wikipedia.org/wiki/Public_key_infrastructure).)

“An alternative approach to the problem of public authentication of public key information ... which however does not deal with public authentication of public key information, is the simple public key infrastructure (“**SPKI**”) that grew out of 3 independent efforts to overcome the complexities of X.509 and PGP’s web of trust. SPKI does not bind people to keys, as the key is what is trusted, rather than the person. SPKI does not use any notion of trust, as the verifier is also the issuer.

This is called an "authorization loop" in SPKI terminology, where authorization is integral to its design."

(See [http://en.wikipedia.org/wiki/Public\\_key\\_infrastructure](http://en.wikipedia.org/wiki/Public_key_infrastructure).)

SPKI specification defines an authorization certificate format, providing for the delineation of privileges, rights or other such attributes (called authorizations) and binding them to a public key. [SPKI] does not define a role for a commercial Certificate Authority (CA). In fact, one premise behind SPKI is that a commercial CA serves no useful purpose.

(See [http://en.wikipedia.org/wiki/Simple\\_public\\_key\\_infrastructure](http://en.wikipedia.org/wiki/Simple_public_key_infrastructure).)

*B. No Basis Exists for the Hypothetical Combination of Saito and Micall*

Saito is directed to a privacy enhanced service scheme utilizing Simple Public Key Infrastructure (SPKI). Saito describes his privacy-enhanced access control system provides the useful property of being "light and efficien[t]," specifically stating the following:

"Since public key is not mapped to ID in an SPKI certificate, public key can be generated for a service or a set of services and discarded after its usage or lifetime. This disposable key scheme alleviates the management of public keys."

(Saito, pg. 302, second column.)

Saito describes another useful property of his privacy-enhanced access control system as being "self-verifiable," specifically stating the following:

"In the SPKI scheme, there is a chain of verification: without a server's or third party's help, clients can verify certificates by themselves."

(Saito, pg. 302, second column.)

In contrast to the SPKI-based system of Saito, Micall is directed to a traditional PKI-based system involving a certificate authority (CA), wherein an intermediary (a "witness") processes authenticated certificate information to construct authenticated deduced information.

## EXPEDITED PROCEDURE

Such a witness system enables users to save transmission costs of certificate information (e.g., reducing need to transmit a long Certificate Revocation List (CRL), or search the CRL, to establish whether a given certificate has been revoked). An advantage of a witness system according to Micall is that, in comparison to direct communication with a CA, the intermediary provides much shorter answers when authenticating the status of issued certificates. (Micall, col. 8, lines 38-45.)

To support the hypothetical combination of Micall and Saito, the examiner stated:

“It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure [of Saito] to include reissuing valid SPKI certificates such as that taught by Micall in order [to] reduce processing overhead by reissuing valid certificate instead of generating a new certificate.”

(March 9, 2009 Office Action, page 3).

The foregoing rationale advanced by the examiner for combining Micall and Saito fails in multiple respects.

First, Saito specifically relates to a *SPKI-based* system (i.e., lacking a Certificate Authority), whereas Micall specifically relates to a *PKI-based* system that requires a Certificate Authority. Various fundamental differences between SPKI-based and PKI-based systems are identified hereinabove, but apparently have been overlooked by the examiner. For example, Micall requires a Certificate Authority, whereas Saito specifically does not require help from a server or third party (e.g., a Certificate Authority) to verify certificates. (See Saito, pg. 302, second column.) Given the fundamental differences between the two references, there is no indication that the PKI-based system of Micall would be compatible with the SPKI-based system of Saito to produce an operative combined system. A proposed combination of references that would produce a “seemingly inoperative” system cannot support a *prima facie* case of obviousness under 35 U.S.C. 103<sup>3</sup>. Accordingly, the proposed combination of Micall and Saito is not supportable.

---

<sup>3</sup> The Federal Circuit and its predecessor court have repeatedly held that **if references taken in combination would produce a ‘seemingly inoperative’ device, then such references teach away from the combination** and cannot serve as predicates for a *prima facie* case of obviousness. *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 60

Second, Saito specifically his SPKI system as being advantageous because it utilizes a disposable key scheme that alleviates the management of public keys (See Saito, pg. 302, second column.) This directly contradicts the examiner's assertion that one skilled in the art would combine Micall with Saito to reduce processing overhead, since addition of Micall's PKI-based complex key management system (i.e., requiring a Certificate Authority) would increase processing overhead. The obviousness rejections premised on the hypothetical combination of Saito and Micall are erroneous for at least the reason that the examiner has failed to consider portions of Saito that teach away from the combination<sup>4</sup>. Given such teaching away, the examiner's rationale supporting the hypothetical combination of references does not embody "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness," as required by the Supreme Court in *KSR International Co. v. Teleflex Inc.*, 127 S.Ct 1727, 167 L.Ed.2d 705, 82 USPQ2d 1385, 1396 (2007).

Each of claims 1, 22, 29, 30, 31, and 32 is allowable over Saito for at least the reason that Saito fails to disclose the feature of "wherein the concealing data remains fixed for reissued associations." As the rejections of Applicants' independent claims 1, 22, 29, 30, 31, and 32 under 35 U.S.C. 103 are all premised on the hypothetical combination of Micall and Saito, and it has been demonstrated that such hypothetical combination of Micall and Saito is insupportable, no basis remains for maintaining such claim rejections.

Allredge fails to remedy the above-identified lack of support for combining Micall and Saito, or to remedy the deficiencies of Saito in disclosing all elements of Applicants' independent claims 1, 22, 29, 30, 31, and 32.

---

USPQ2d 1001, 1010 (Fed. Cir. 2001); *Tec Air, Inc. v. Denso Mfg. Mich. Inc.*, 192 F.3d 1353, 52 USPQ2d 1294, 1298 (Fed. Cir. 1999) (proposed combination of references that would be inoperable for intended purpose supports teaching away from combination); *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) (inoperable modification teaches away); *In re Spinnoble*, 405 F.2d 578, 587, 160 USPQ 237, 244 (C.C.P.A. 1969) (references teach away from combination if combination produces seemingly inoperative device).

<sup>4</sup> In considering a reference for its effect on patentability, the reference is required to be considered in its entirety, including portions that teach away from the invention under consideration. Simply stated, the prior art must be considered as a whole. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984) (emphasis added); MPEP § 2141.02. "It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art." *Application of Wesslau*, 353 F.2d 238, 241 (C.C.P.A. 1965); *Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve*, 796 F.2d 443, 448 (Fed. Cir. 1986), *cert. denied*, 484 U.S. 823 (1987).

## EXPEDITED PROCEDURE

Accordingly, withdrawal of the rejections of Applicants' independent claims 1, 22, 29, 30, 31, and 32 is warranted, and is respectfully requested. Since dependent claims inherently include all of the features of the claims on which they depend<sup>5</sup>, all claims depending (whether directly or indirectly) from independent claims 1, 22, 29, 30, 31, and 32 are likewise patentably distinguished over the cited art. Applicants respectfully submit that all pending claims are in form and condition for allowance.

### CONCLUSION

In light of the foregoing, Applicants respectfully submit that all of the now pending claims are in condition for allowance. As all issues raised by the Examiner have been addressed, issuance of a notice of allowance is earnestly solicited.

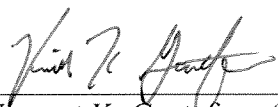
Please direct all correspondence in this application to:

Kevin C. Ecker (Reg. No. 43,600)  
Senior IP Counsel

Philips Intellectual Property & Standards.  
P.O. Box 3001, Briarcliff Manor, NY 10510-8001 USA.  
Phone: +1 (914) 333-9618.  
Fax: +1 (914) 332-0615.  
E-mail: kevin.ecker@philips.com

Respectfully submitted,

Dated: May 11, 2009

By:   
Vincent K. Gustafson (Reg. No. 46,182)

INTELLECTUAL PROPERTY/  
TECHNOLOGY LAW  
P.O. Box 14329  
Research Triangle Park, North Carolina 27709  
Phone: 919-419-9350  
Fax: 919-419-9354

---

<sup>5</sup> 35 U.S.C. 112, fourth paragraph.